THAT WHICH IS CLAIMED:

1. A method for protecting against the unauthorized use of software originally installed upon a computer from a medium having a radio frequency device, comprising:

obtaining a first access-control code from a memory device resident within the computer, wherein the access control code is associated with the computer, a smart card, and the radio frequency device;

obtaining a second access-control code resident on the smart card, wherein the access control code is associated with the computer, the smart card, and the radio frequency device; and

allowing software to execute when the first access-control code and the second access-control code are the same.

2. The method of Claim 1, further comprising installing the software on the computer.

3. The method of Claim 2, wherein installing the software on the computer comprises obtaining the first access-control code, obtaining the second access-control code, comparing the first and the second access-control codes, and if the first and second access control codes are the same, writing the access control code to the radio frequency device associated with the medium.

4. The method of Claim 2, wherein installing the software on the computer comprises obtaining the first access control code, obtaining the second access control code, comparing the first and second access control codes, and, if the first and second access control codes are identical, writing the access control code to the medium that embodies the software.

5. A method for protecting against the unauthorized installation of software resident on a medium, comprising:

obtaining a first access-control code from a memory device resident within a computer;

obtaining a second access-control code resident on a smart card;

obtaining any third access-control code associated with the medium;

comparing the first access-control code and the second access-control code; and

allowing installation of the software when the first access-control code and the second access-control code are the same and the medium is without any third access-control code.

6. The method of Claim 5, wherein installing the software comprises writing the first access-control code to a programmable device associated with the medium when the first access-control code and the second access-control code are the same and the medium is otherwise without any third access-control code.

7. The method of Claim 5, further comprising allowing installation of the software when the third access-control code and the second access-control code are the same.

8. The method of Claim 7, further comprising writing the first access-control code to the memory device resident on the computer when the second access-control code and the third access-control code are the same.

9. A method for allowing a user to reinstall onto a computer protected software resident on a medium, comprising:

obtaining a first access-control code resident on a smart card;

obtaining a second access-control code associated with the medium;

comparing the first access-control code and second access-control code; and

installing the protected software on the computer if the first access-control code and second access-control code are the same.

10. The method of Claim 9, further comprising writing the first access-control code to a memory device of the computer.

11. The method of Claim 9, further comprising ejecting the medium if the first access-control code and second access-control code are not the same

12. A system for protecting against the unauthorized use and unauthorized installation of software, comprising:

a computer having a memory device;

a smart card drive communicatively connected to the computer, wherein said smart card includes an access-control code that is capable of being read by said computer from the smart card; and

an optical disc drive communicatively connected to the computer for receiving an optical disc having a radio frequency device embodied therein, said optical disc drive comprising a radio frequency drive capable of reading an access-control code from the radio frequency device.

13. The system of Claim 12, wherein the radio frequency drive is also capable of writing an access-control code to the radio frequency device.

14. A computer-readable storage medium encoded with processing instructions for implementing a method for protecting against the unauthorized installation of software, said processing instructions directing a computer to perform the steps of:

obtaining a first access-control code from a memory device resident within a computer;

obtaining a second access-control code resident on a smart card;

obtaining any third access-control code resident on a programmable device that is associated with the medium;

comparing the first access-control code, the second access-control code, and the third access-control code; and

allowing installation of the software when the first access-control code and the second access-control code are the same and the programmable device associated with the medium is without any third access-control code.

15. The computer-readable storage medium of Claim 14 further comprising processing instructions directing a computer to perform the step of writing the first access-control code to the programmable device associated with the medium when the first access-control code and the second access-control code are the same and the medium is otherwise without any third access-control code.

16. A computer-readable storage medium encoded with processing instructions for implementing a method for protecting against the unauthorized installation of software, said processing instructions directing a computer to perform the steps of:

obtaining a first access-control code from a memory device resident within a computer;

obtaining a second access-control code resident on a smart card;

obtaining any third access-control code resident on a programmable device that is associated with the medium;

comparing the first access-control code, the second access-control code, and the third access-control code; and

allowing installation of the software when the first access-control code and the second access-control code and the third access-control code are the same.

17. A computer-readable storage medium encoded with processing instructions for implementing a method for protecting against the unauthorized use of software originally installed upon a computer from a medium having a radio frequency device, said processing instructions directing a computer to perform the steps of:

obtaining a first access-control code from a memory device resident within the computer, wherein the access control code is associated with the computer, a smart card, and the radio frequency device;

obtaining a second access-control code resident on the smart card, wherein the access control code is associated with the computer, the smart card, and the radio frequency device; and

allowing software to execute when the first access-control code and the second access-control code are the same.

18. The computer-readable storage medium of Claim 17 further comprising processing instructions directing a computer to perform the step of installing the software on the computer.

19. The computer-readable storage medium of Claim 18 wherein the processing instructions directing a computer to perform the step of installing the software comprises obtaining the first access-control code, obtaining the second access-control code, comparing the first and the second access-control codes, and if the first and second access control codes are the same, writing the access control code to the radio frequency device associated with the medium.